

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-087336

(43)Date of publication of application : 20.03.2003

(51)Int.Cl.

H04L 12/66

G06F 13/00

H04L 29/06

(21)Application number : 2001-274419

(71)Applicant : HITACHI LTD

(22)Date of filing : 11.09.2001

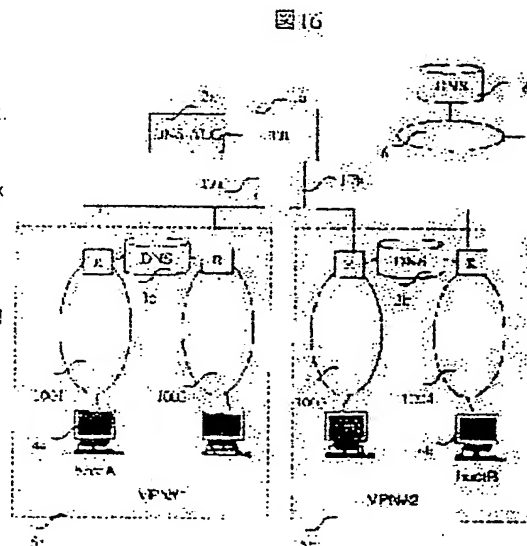
(72)Inventor : INAI HIDENORI
TAKEDA SACHIKO
HAYASHI MASAYA
TAKEUCHI TAKAAKI
SENOO TAKAMITSU

(54) ADDRESS CONVERSION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To solve a problem of a conventional technology that cooperation between the DNS-ALG (Domain Name Service-Application Level Gateway) and the Twice NAT (Network Address Translation) is not scalable because an increased size of the conversion table is required.

SOLUTION: A translator 1a has a communication means with a DNS-ALG 2. The DNS-ALG 2 detects a DNS inquiry to a called party terminal 4b and converts it once into the IPv6. The DNS-ALG 2 converts a called destination virtual IPv6 address resulting from attaching a virtual IPv6 prefix to the real address of the IPv4 acquired from a DNS server 3b of the called party terminal 4b into a called party virtual IPv4. Thus, cooperation of the DNS-ALG of the IPv6 base and the translator 1 can relieve the processing load on the DNS-ALG 2 and reduce a large capacity conversion table. Interconnection is thus attained among a plurality of VPNs without the need for replacing the existing VPN.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998.2003 Japan Patent Office

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-87336

(P2003-87336A)

(43) 公開日 平成15年3月20日 (2003.3.20)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-コ-ド [*] (参考)
H 0 4 L 12/66		H 0 4 L 12/66	E 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 B 5 K 0 3 0
H 0 4 L 29/06		H 0 4 L 13/00	3 0 5 B 5 K 0 3 4

審査請求 未請求 請求項の数20 O L (全 20 頁)

(21) 出願番号 特願2001-274419(P2001-274419)

(22) 出願日 平成13年9月11日 (2001.9.11)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 井内 秀則

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(72) 発明者 武田 幸子

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

(54) 【発明の名称】 アドレス変換方法

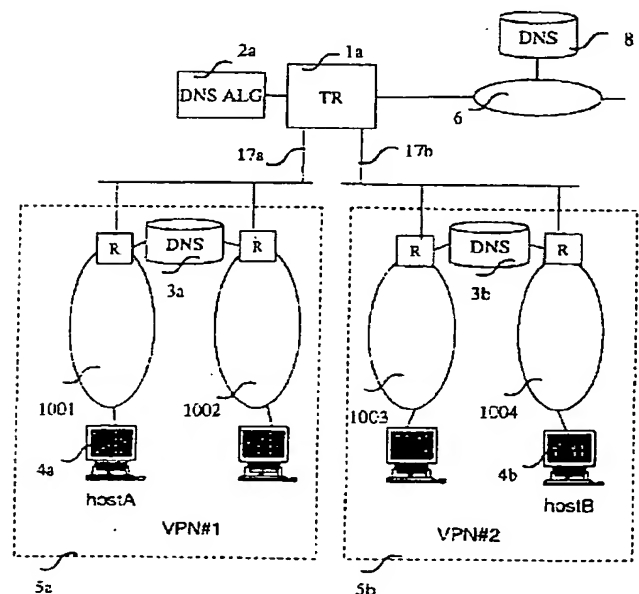
(57) 【要約】 (修正有)

【課題】 DNS-ALGとTwice NATの連携は、変換テーブルが増大するため、スケーラブルではない。

【解決手段】 トランスレータ1aはDNS-ALG2との通信手段を備える。DNS-ALG2は、着側端末4bに対するDNS問い合わせを検出し、一度IPv6に変換する。DNS-ALG2は、着側端末4bのDNSサーバ3bから取得したIPv4の実アドレスに仮想IPv6プレフィックスを付加した着信先仮想IPv6アドレスを着信先仮想IPv4に変換する。

【効果】 IPv6ベースのDNS-ALGとトランスレータ1の連携により、DNS-ALG2の処理負荷の軽減と大容量変換テーブルの削減を可能にする。既存のVPNを置きかえることなく、複数のVPN間で相互接続が可能になる。

図16



【特許請求の範囲】

【請求項1】第1のプロトコルPに従う複数の網A1、A2と、第2のプロトコルQに従う網Bと、上記網A1と網Bを接続する第1のアドレス変換装置と、上記網A2と網Bを接続する第2のアドレス変換装置と、サーバ装置を有する通信網におけるアドレス変換方法であって、

上記第1及び第2のアドレス変換装置はプロトコルP、Qを相互に変換する手段と、上記サーバ装置との通信手段と、上記サーバ装置と連携してプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する手段を有し、上記サーバ装置は、上記アドレス変換装置がプロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置と通信する手段を有し、

上記第1のアドレス変換装置が上記変換情報を参照してプロトコルPとプロトコルQを相互に変換したのち、上記第2のアドレス変換装置がプロトコルQとプロトコルPを相互に変換することにより、プロトコルPに従う網A1がプロトコルPに従う網A2と通信することを特徴とするアドレス変換方法。

【請求項2】あるプロトコルPに従う網と上記プロトコルPと異なるプロトコルQに従う網とを接続するアドレス変換装置において、プロトコルP、Qを相互に変換する手段と、プロトコルP、Qを相互に変換するために必要な情報を有するサーバ装置と通信する手段と、上記サーバ装置と連携してプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する手段と、プロトコルP、Qを相互に変換する際に上記作成した変換情報を参照することを特徴とするアドレス変換装置。

【請求項3】あるプロトコルPに従う複数の網と上記プロトコルPと異なるプロトコルQに従う網とを、プロトコルP、Qを相互に変換する複数のアドレス変換装置で接続する通信網におけるサーバ装置において、上記アドレス変換装置においてプロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置と通信する機能と、上記アドレス変換装置にプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備えるサーバ装置。

【請求項4】あるプロトコルPに従う複数の網A1、A2をアドレス変換装置で接続する通信網において、アドレス変換装置はプロトコルPを内部でプロトコルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段と、上記サーバ装置と連携して、プロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する機能とを備え、上記サーバ装置は、上記アドレス変換装置においてプロトコルP、Qを相互に変換するために必要な変換情報と、上記プロトコルPに従う網対応にプロトコルQに従うアドレスと、上記変換情報を作成するために他のサーバ装置、も

しくは、上記サーバ装置の別のアドレスと通信する機能を備え、

プロトコルPに従う網A1からプロトコルPに従う網A2への通信は、上記アドレス変換装置が上記変換情報を参照してプロトコルPに従うアドレスからプロトコルQに従うアドレスに変換し、変換されたプロトコルQに従うアドレスをさらにプロトコルPに従うアドレスに変換することとを特徴とする通信網。

【請求項5】上記アドレス変換装置が上記プロトコルPに従う複数の網をレイヤ2の情報により識別する機能をさらに有し、

上記アドレス変換装置が通信要求を受信するとレイヤ2の情報によりプロトコルPに従う網を特定し、プロトコルPからプロトコルQに変換することを特徴とする請求項4に記載の通信網。

【請求項6】上記プロトコルPに従う複数の網が、多重装置に接続され、上記多重装置と上記アドレス変換装置が複数の回線で接続され、

上記多重装置が上記プロトコルPに従う網をレイヤ2の情報により識別する機能を備え、

上記多重装置が上記プロトコルPに従う網から通信要求を受信するとレイヤ2の情報によりプロトコルPに従う網を特定し、対応する回線を用いて、上記アドレス変換装置に通信要求を送信する請求項4に記載の通信網。

【請求項7】あるプロトコルPに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項4に記載の通信網。

【請求項8】あるプロトコルPに従う複数の網接続するアドレス変換装置において、プロトコルPを内部でプロトコルQに相互に変換する機能と、

サーバ装置と通信するために必要な情報と通信手段と、上記プロトコルPに従う網対応にプロトコルQに従うアドレスと、プロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置、もしくは、上記サーバ装置の別のアドレスと通信する機能を備えるサーバ装置と連携して、プロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する機能を備えるアドレス変換装置。

【請求項9】上記プロトコルPに従う複数の網をレイヤ2の情報により識別する機能をさらに備え、通信要求を受信するとレイヤ2の情報によりプロトコルPに従う網を特定し、プロトコルPからプロトコルQに変換する手段を備える請求項8に記載のアドレス変換装置。

【請求項10】あるプロトコルPに従う複数の網をアドレス変換装置で接続する通信網において、上記アドレス変換装置は、内部でプロトコルPをプロト

コルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段を備え、

上記プロトコルPに従う網対応にプロトコルQに従うアドレスと、プロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために他のサーバ装置、もしくは、上記サーバ装置の別のアドレスと通信する手段と、

上記アドレス変換装置にプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備える通信網。

【請求項11】あるプロトコルPに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項10に記載の通信網。

【請求項12】あるプロトコルPに従う複数の網をアドレス変換装置で接続する通信網において、アドレス変換装置は、内部で上記プロトコルPをプロトコルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段を備え、上記プロトコルP、Qを相互に変換するために必要な変換情報と、

上記変換情報を作成するために、あるプロトコルPに従う網の識別情報とプロトコルPに従う網に属するサーバ装置に対して付与されたプロトコルQに従うアドレスの対応関係を管理し、あるプロトコルPに従う網の名前解決要求を受信すると、上記対応関係を参照して他のサーバ装置と通信する手段と、

上記アドレス変換装置にプロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備えるサーバ装置。

【請求項13】あるプロトコルPに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項12に記載のサーバ装置。

【請求項14】あるプロトコルPに従う複数の網をアドレス変換装置で接続する通信網において、アドレス変換装置はプロトコルPを内部でプロトコルQに相互に変換する機能と、サーバ装置と通信するために必要な情報と通信手段と、上記サーバ装置と連携して、プロトコルPでのアドレスとプロトコルQでのアドレスの対応関係を含む変換情報を作成する機能を備え、上記サーバ装置は、上記アドレス変換装置においてプロトコルP、Qを相互に変換するために必要な変換情報と、上記変換情報を作成するために、あるプロトコルPに従う網の識別情報とプロトコルPに従う網に属するサーバ装置に対して付与されたプロトコルQに従うアドレスの対応関係と、あるプロトコルPに従う網の名前解決要求を受信すると、上記対応関係を参照して他のサーバ装置と通信する手段と、

上記アドレス変換装置にプロトコルPでのアドレスとプ

ロトコルQでのアドレスの対応関係を含む変換情報の作成を要求する手段を備え、

プロトコルPに従う網A1からプロトコルPに従う網A2への通信は、上記アドレス変換装置が上記変換情報を参照してプロトコルPに従うアドレスからプロトコルQに従うアドレスに変換し、変換されたプロトコルQに従うアドレスをさらにプロトコルPに従うアドレスに変換することとを特徴とするアドレス変換方法。

【請求項15】あるプロトコルPに従う複数の網が異なるアドレス変換装置に接続され、アドレス変換装置がプロトコルQに従う網に接続される通信網における請求項14に記載のアドレス変換方法。

【請求項16】第1の網と、該第1の網と通信可能な第2の網と、該第2の網と通信可能な第3の網と、上記第1の網と第2の網を接続する第1のアドレス変換装置と、上記第2の網と第3の網を接続する第2のアドレス変換装置とを有し、

上記第1のアドレス変換装置は、上記第1の網で使われているアドレスに上記第1の網を示すプレフィックスを付加した第1仮想アドレスを、上記第2の網を介して上記第2のアドレス変換装置に送り、

上記第2のアドレス変換装置は、上記第1仮想アドレスを上記第3の網で使われていないアドレスである第2仮想アドレスに変換して、上記第3の網に送り、上記第1仮想アドレスと上記第2仮想アドレスとの対応関係を記憶することを特徴とする情報網。

【請求項17】上記第3の網から送られてきた上記第2仮想アドレスを、上記対応情報に基づいて上記第1仮想アドレスに変換し、該第1仮想アドレスから上記プレフィックスを削除して、上記第1の網に送ることを特徴とする請求項16記載の情報網。

【請求項18】上記第1の網は第1のプロトコルに従い、上記第2及び第3の網は第2のプロトコルに従うことを特徴とする請求項17記載の情報網。

【請求項19】第1の網と第2の網の間に配置され、該第1の網と第2の網の間の通信を仲介する通信装置であって、

上記第1の網から送られてきた上記第1の網で使われている元アドレスを受信し、該元アドレスにプレフィックスを付加した第1仮想アドレスを形成し、該第1仮想アドレスを上記第2の網に送出し、

上記第2の網から送られてきた上記第1仮想アドレスを受信し、該第1仮想アドレスからプレフィックスを削除して元アドレスを形成し、該元アドレスを上記第1の網に送出することを特徴とする通信装置。

【請求項20】上記第2の網から送られてきた第1アドレスを、上記第1の網で使われていない第2アドレスに変換し、上記第1の網に送出し、上記第1アドレスと第2アドレスの関連を変換情報として保持し、

上記第1の網から送られてきた第2アドレスを、上記変換情報にもとづいて上記第1アドレスに変換し、該第1アドレスを上記第2の網に送出することを特徴とする請求項19記載の通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は同一のプロトコルに従う網、あるいは、異なるプロトコルに従う網を相互接続する方式に関する。

【0002】

【従来の技術】例えばプライベート網どうしをインターネットで接続し、ひとつのVPN(Virtual Private Network)として見せる技術として、Twice NAT(Network Address Translation)技術を使う方法(<http://www.ietf.org/rfc/rfc2663.txt>のpp12-13参照)や、トンネル技術を使う方法(<http://www.ietf.org/rfc/rfc2663.txt>のpp22参照)が知られている。いずれも基本的にIPパケットのヘッダ情報をIPv4とIPv4とで相互に変換する。例えば基本的なNATは、プライベートIPv4アドレスとパブリックIPv4アドレスの変換を行う。NATを2つ直列に接続した、いわゆるTwice NAT技術を実装したルータはTwice NATルータと呼ばれる。従来の基本NAT、双方向NATでは、送信元アドレス、もしくは着信先アドレスのどちらか一方を書き換えていたが、Twice NAT技術では、Twice NATルータで接続された二つの領域間をデータグラムが通過する時点で、送信元アドレスと着信先アドレスの両方を書き換える。Twice NATは、プライベートネットワーク内のアドレス空間とパブリック空間のアドレス空間が衝突している場合に使用されることが多い。あるサイトのアドレス付けを誤って他のサイトのパブリックアドレスをつけてしまった場合、あるプロバイダからアドレスをもらっていたが、他のプロバイダに乗り換えた後もしばらくは、以前のプロバイダから割り当ててもらったアドレスを使い続け、そのプロバイダが別ユーザに対して同じアドレスを割り当ててしまった場合に、アドレス衝突が発生する。アドレス衝突を解決するためには、Twice NATは以下のように動作する。プライベート領域内のHost-Aがパブリック領域内のHost-Xと通信をはじめる場合には、Host-AはHost-XのDNSアドレス問い合わせパケットを送信する。DNS-ALG(Domain Name Service - Application Level Gateway)がこのパケットを捕捉し、かつHost-Xに対するアドレスをプライベート領域内でルーティング可能なアドレス(Host-XPRIME)に変換してHost-Aに返す。DNSアドレス解決が終了したらHost-AはHost-XPRIMEとの間で通信を開始する。このパケットがTwice NATを通過する時点で、送信元アドレスがNATの持つアドレスに書き換えられ、着信先アドレスはHost-Xに書き換わる。Host-Xからの返信パケットもこれと同様の変換が行われる。上記DNS-ALGの動作詳細については、<http://www.ietf.org/rfc/rfc2693.txt>に詳細が記載されている。Twice

NATを使用する方法は、インターネットを介して多数のホストどうしで通信する場合に、大容量の変換テーブルが必要になる。特定のIPアドレスを使うアプリケーションが多い場合には、上記のようにDNSアドレス問い合わせをトリガにしたNATによるダイナミックなアドレス変換ができないという問題がある。上記の問題点を解決するために、NAT技術ではなくトンネル技術を用いて二つの領域を相互接続する方法がある。トンネル技術を用いる方法は、接続対象になっている二つの網内の端末が同一のアドレスを持つ場合には、同一のアドレスを有する端末間では通信ができない、異なる接続する二つの領域が同一のサブネットを持たないといけないという制限がある。しかしながら、Twice NAT使用時のように大容量の変換テーブルを持つ必要はないので、インターネットを介して同一のサブネット空間を共有するPrivate VLAN(Virtual LAN)どうしを相互接続する技術としてはトンネル技術が使われることが多い。以上の例は、ある端末が属する網と通信相手の端末が属する網の通信プロトコルが同一の場合に使われる技術である。ある端末が属する網と通信相手の端末が属する網の通信プロトコルが異なる場合には、例えばプロトコルとしてIPv4を用いる網(以下IPv4網と呼ぶ)とInternet Protocol version 6を使用する網(以下IPv6網と呼ぶ)を接続する変換方式としてNAT-PT(<http://www.ietf.org/rfc/rfc2766.txt>のpp6-18、および[rfc2765.txt](http://www.ietf.org/rfc/rfc2765.txt)のpp9-22参照)、SOCKS64(<http://search.ietf.org/internet-drafts/draft-ietf-ngt-rans-socks-gateway-05.txt>参照)等が知られている。いずれも基本的にIPパケットのフォーマットをIPv4とIPv6とで相互に変換する。例えば、IPv4アドレスとIPv6アドレスの変換を行う。この変換を行う装置を以下トランスレータと呼ぶ。トランスレータでは変換のために、変換の前にIPv4アドレスとIPv6アドレスの対応関係を作成し、保持しておく必要がある。この対応関係を通信が発生するたびに動的に作成する場合に、そのきっかけとしてDNS(ドメインネームシステム)の名前解決が利用される(アスキー出版、インターネットRFC事典、pp323-329を参照)。DNSはウェブのURLのような人間にわかりやすい名前(文字列)を、IPアドレスに変換するシステムである。以下名前をIPアドレスに変換する操作を名前解決と呼ぶ。今日ではインターネット上のほぼすべてのアプリケーションがこのDNSを利用して通信相手のIPアドレスを取得している。NAT、及びトランスレータはこの事実を利用し、通信開始にあたってやり取りされるDNSのメッセージを常に監視しており、名前解決の要求メッセージを変換情報(IPアドレスの対応関係等)を作成するきっかけとする。具体的には、IPv6端末がある名前について名前解決を行ったとき、その応答であるIPアドレスがIPv4だった場合、このIPv4アドレスをIPv6アドレスに書き換えてIPv6端末に送り返す。そして、書き換える前のIPv4アドレスと書き換えたIPv6アドレスを対応付ける。つ

まりDNS-ALGは名前解決の応答メッセージを横取りして書き換え、この書き換える前と書き換えた情報をもとに変換情報を作成する。ここで動的に作成された変換情報は一時的なものであるから、通信が終了すると廃棄される。DNS-ALGが保持する、IPv4アドレスとIPv6アドレスの対応関係、若しくはIPv4アドレスとIPv6アドレスの対応関係は通信終了とともに廃棄され、通信ごとに異なるものが使用される。すなわち、名前解決の応答メッセージを書き換える内容が通信ごとに異なる。したがって、名前解決を要求した端末から見ると、同じ名前に対して異なるIPアドレスを取得することとなる。

【0003】このように、DNS-ALGとトランスレータの連携は、インターネット上のほぼすべてのアプリケーションがこのDNSを利用して通信相手のIPアドレスを動的に取得している状況において、IPv6ネットワークとIPv4ネットワークを接続するために必須の技術である。また、DNS-ALGとTwice NATの連携は、パブリックアドレスの移行時に発生するIPv4プライベートアドレスの競合問題を解決する技術である。

【0004】

【発明が解決しようとする課題】上述した通り、トンネル方式によるVPNの相互接続は、IPアドレスの衝突に対処できないという課題がある。また、DNS-ALGとTwice NATの連携は、パブリックアドレスの移行時に発生するIPv4プライベートアドレスの競合問題を解決する技術である。しかし、DNS-ALGとTwice NATの連携は、アドレス変換テーブルが大きく、スケーラブルでないという課題がある。一般的に、VPN間の相互接続は、VPNのエッジにDNS-ALGとTwice NATを設置し、実現することが多い。しかし、相互接続するVPNの数が多い場合、アドレス変換テーブルが大きくなるため、サービスの提供が困難であるという課題がある。本発明の目的は、ある端末が属する網と通信相手の端末が属する網の通信プロトコルが同一の場合に、両方のアドレス空間が衝突した場合にも、両方の端末どうしの通信を可能にすることにある。本発明の他の目的は、ある端末が属する網と通信相手の端末が属する網の通信プロトコルが異なる場合には、基本トランスレーションによって、両方の端末どうしの通信を可能にする、スケーラブルで実用的なアドレス変換装置を提供することにある。

【0005】本発明はIPv6ベースのDNS-ALGとTwice NAT-PTの連携によって、従来のTwice NATによるアドレス変換で必要な変換情報を動的に作成する場合に必要であった、着側の端末に対する仮想アドレスを生成するDNS-ALGの処理負荷の軽減と大容量変換テーブルの削減を可能にする。

【0006】本発明によるIPv6ベースのDNS-ALGとTwice NAT-PTをプロバイダが一括管理し、トランスレータに複数のVPNを収容すれば、既存のVPNを置きかえることなく、複数のVPN間での相互接続が可能になる。

【0007】

【課題を解決するための手段】従来の、NAT-PTに代表されるプロトコル変換方式に加え、少なくとも以下の2点の手段を備える。すなわち、①複数のトランスレータがもつ、IPv4アドレスとIPv6アドレスの対応関係に代表されるアドレス変換に必要な変換情報を管理するDNS-ALG装置を備え、②各トランスレータは前記DNS-ALG装置と通信を行うためのプロトコルを備える。

【0008】Twice NAT-PTによるアドレス変換で必要な変換情報を動的に作成するため、DNS-ALG装置は、発側の端末からの送信される着側端末に対するDNS問い合わせを、装置の内部では一度IPv6に変換する。DNS-ALG装置は、着側のIPv4 DNSサーバにおける問い合わせで取得したIPv4の実アドレスに仮想IPv6プレフィックスを付加したIPv6アドレスを着側の端末に対する仮想IPv6アドレスとして使用する。仮想IPv6アドレスを仮想IPv4アドレスに変換し、発側端末に通知する。この方式をとることによって、従来のTwice NAT方式と比較すると、変換回数が一回少なくなると同時に変換テーブルのサイズを小さくすることができる。さらに、③各トランスレータはL2情報を活用してプロトコル変換を行う手段を備えてもよい。IPアドレス以外にもMACアドレスに代表されるL2情報を用いたプロトコル変換を行う手段を備えることによって、1つの物理回線上に複数のVPNを多重することが可能になる。このような発明を適用した情報網は、第1の網と、第1の網と通信可能な第2の網と、第2の網と通信可能な第3の網と、第1の網と第2の網を接続する第1のアドレス変換装置と、第2の網と第3の網を接続する第2のアドレス変換装置とを有し、第1のアドレス変換装置は、第1の網で使われているアドレスに第1の網を示すプレフィックスを付加した第1仮想アドレスを、第2の網を介して第2のアドレス変換装置に送り、第2のアドレス変換装置は、第1仮想アドレスを第3の網で使われていないアドレスである第2仮想アドレスに変換して第3の網に送り、第1仮想アドレスと第2仮想アドレスとの対応情報を記憶する。また、第3の網から送られてきた第2仮想アドレスを、対応情報に基づいて第1仮想アドレスに変換し、第1仮想アドレスからプレフィックスを削除して、第1の網に送る。この場合、第1の網は第1のプロトコルに従い、第2及び第3の網は第2のプロトコルに従うこととしてもよい。また、変換されるアドレスは、送信元アドレスまたは送信先アドレスとしてもよい。

【0009】このような網に用いられる通信装置としては、第1の網と第2の網の間に配置され、第1の網と第2の網の間の通信を仲介する通信装置であって、第1の網から送られてきた第1の網で使われている元アドレスを受信し、元アドレスにプレフィックスを付加した第1仮想アドレスを形成し、第1仮想アドレスを第2の網に送出し、第2の網から送られてきた第1仮想アドレスを

受信し、第1仮想アドレスからプレフィックスを削除して元アドレスを形成し、元アドレスを第1の網に送出する。

【0010】また、他の通信装置は、第2の網から送られてきた第1アドレスを、第1の網で使われていない第2アドレスに変換し、第1の網に送出し、第1アドレスと第2アドレスの関連を変換情報として保持し、第1の網から送られてきた第2アドレスを、変換情報にもとづいて第1アドレスに変換し、第1アドレスを第2の網に送出する。

【0011】

【発明の実施の形態】本発明の第1の実施の形態を図面を用いて説明する。

【0012】図1は、本発明によるVPN間接続サービスを提供するネットワークの構成例を示す。VPN間接続サービスを提供するネットワークは、VPN5とIP網6から構成される。VPN5は、DNSサーバ3を備える。VPN5aは、例えば企業の拠点(1001、1002)を仮想的に相互に接続する。本実施例では、VPN5は、IPv4プライベートアドレスを利用する。1つのVPN内においてはIPアドレスは重複しないが、異なるVPNの間でIPアドレスは重複してもよい。IP網6はDNSサーバ8を備える。本実施例では、IP網6はIPv6アドレスを利用する。

【0013】VPN5とIP網6は、トランスレータ1(TR)で接続する。トランスレータ1は、IPv6アドレスとIPv4アドレスの変換機能と、DNS-ALG2と通信する手段を備える。DNS-ALG2は、複数のトランスレータがもつIPv4アドレスとIPv6アドレスの対応関係に代表されるアドレス変換に必要な変換情報を管理し、DNSの問い合わせやその返信のパケットの中身を書き換える手段を備える。第1の実施の形態において、DNS-ALG2は、VPN5毎に存在する。

【0014】図2は、トランスレータ1の構成例を示す。トランスレータ1は、回線(17a、17b、17c、17n)を収容するインタフェース部(IF)(16a、16b、16c、16n)と、メモリ14と、CPU15とを、スイッチまたはバス18で接続する構成となっている。メモリ14は、アドレスの変換に必要な情報11やデータパケットを変換するためのプログラム13や、DNS-ALG2からの変換エントリ登録要求を処理するためのプログラム12が格納されている。変換情報記憶部11は、図9に示す仮想プレフィックス管理テーブル300と図11に示す変換情報テーブル500を備える。

【0015】図9は、仮想プレフィックス管理テーブル300のテーブル構成を示す。本テーブルは、トランスレータ1の回線番号ごとに生成された複数のエントリ(300-1~300-n)からなる。各エントリは、回線番号301対応に、仮想プレフィックス302と、変換情報テーブル500へのポインタ303を定義する。

【0016】図11は、変換情報テーブル500のテーブル構成を示す。本テーブルには、IPv4アドレス501とIPv6アドレス502の対応関係が格納される。本テーブルは、VPN毎に生成され(510、520、530)、VPNを収容するトランスレータ1の変換情報記憶部11に格納される。例えば、図1において、VPN#1変換情報テーブル510はトランスレータ1aに、VPN#3変換情報テーブル530はトランスレータ1bに格納される。

【0017】図2へ戻りトランスレータ1の説明を続ける。変換エントリ登録処理12は、変換情報登録要求を処理し、IPアドレスの対応情報を変換情報記憶部11の変換情報テーブル500に格納する。データパケット変換・処理部13は、IPv4パケットを受信すると変換情報記憶部11を検索し、IPv6アドレスをIPv4アドレスに書き換える。また、データパケット変換・処理部13は、IPv6パケットを受信すると、変換情報記憶部11を検索し、IPv4アドレスをIPv6アドレスに書き換える。このとき、IPアドレスのほかにもさまざまな情報を書き換えることが可能である。図4にIPv4パケットフォーマットを示す。図5にIPv6パケットのフォーマットを示す。変換の際にはIPアドレスだけでなく、このフォーマットも変換する。

【0018】図3は、DNS-ALG2の構成例を示す。DNS-ALG2は、回線(24a、24b)を収容するインタフェース部(IF)(23a、23b)と、メモリ22と、CPU21とを、バス25で接続する構成となっている。

【0019】図14と図15に示すシーケンスに従って、図1におけるVPN5aの端末4aがVPN5cの端末4cと通信する場合について説明する。通信開始にあたり、端末4aは端末4cの名前(hostCとする)のアドレスを得るため、DNSサーバ3aに対してDNS問い合わせを行う(101)。DNS問い合わせのパケットフォーマットを図6に示す。図6に示すように、QNAME(421)に名前hostCが、QTYPE(422)に資源レコードのタイプ“A”が記載される。図14に戻り説明を続ける。DNSサーバ3aはこの名前hostCに対応するIPアドレスを知らないため、次のDNSサーバ(DNS-ALG2a)に対してDNS問い合わせを行う(102)。

【0020】DNS-ALG2aは、名前hostCに対するIPアドレスを知らない場合、図12、13に示す処理ルーチン60を起動する。DNS問い合わせのQTYPEが“A”の場合、DNS-ALG2aはQTYPEを“AAAA”に変換する(62、103)。DNS-ALG2aは変換したDNS問い合わせを次のDNSサーバ8に送信し(63、104)、DNS応答を待つ(64)。DNSサーバ8は、次のDNSサーバ(DNS-ALG2b)にDNS問い合わせを送信する(105)。DNS-ALG2bは、名前hostCに対するIPアドレスを知らない場合、図12、13に示す処理ルーチン60を起動する。DNS問い合わせのQTYPEが“AAAA”の場合、QTYPEを“A”に

変換する(81、106)。DNS-ALG2bは変換したDNS問い合わせを次のDNSサーバ3cに送信し(82、107)、DNS応答を待つ(83)。DNSサーバ3cは、名前hostCに対するIPv4アドレス“c”を応答する(84、108)。

【0021】図7にDNSサーバ3cからのDNS応答パケットのフォーマットを示す。図7の43、44、45の詳細フォーマットを図8に示す。NAME(51)に名前hostC、RDATA(54)にIPアドレス“c”が記載される。図14を参照すると、DNS-ALG2bは以後の変換のためにIPv4アドレス“c”をIPv6アドレス“y+c”に書き換える。このIPv6アドレスは、VPN5cに対して割り当てられる仮想的なIPv6プレフィックス(y)+IPv4アドレス(c)で構成される(109)。以降、このアドレスを「着信先仮想IPv6アドレス」と呼ぶ。DNS-ALG2bは、DNS応答のTYPE(52)を“A”から“AAAA”に変換し、RDATA(54)に“y+c”を設定したDNS応答をDNSサーバ8に送信する(85、110)。DNSサーバ8は、DNS-ALG2aに名前hostCに対する着信先仮想IPv6アドレス“y+c”を応答する(65、111)。DNS-ALG2aは、以後の変換のために、このIPv6アドレス“y+c”をIPv4アドレスc'に変換する(112)。このIPv4アドレスは名前hostCに対する仮想的なアドレスで、VPN5aで使用されていないIPアドレスの集合から選ぶ。以降、このアドレスを「着信先仮想IPv4アドレス」と呼ぶ。DNS-ALG2aは、DNS応答のTYPE(52)を“AAAA”から“A”に変換し、RDATA(54)に着信先仮想IPv4アドレスc'を設定したDNS応答をDNSサーバ3a経由で端末4aに送信する(66、115、116)。このとき、y+cとc'の対応付け変換規則を作成し、トランスレータ1aに送信する(67、113)。トランスレータ1aは、変換規則を変換情報記憶部11内のVPN#1変換情報テーブル510に記憶し、DNS-ALG2aに応答を送信する(114)。

【0022】DNS応答を受信した端末4aは端末4cへ向けてIPパケットの送信を始める。これらのパケットの着信先アドレスはc'、送信元アドレスは端末のIPv4アドレスaである(131)。

【0023】トランスレータ1aは、このパケットが到着するとデータパケット変換・処理部13に送る。ここでは、変換情報記憶部11にデータを受信した回線の番号と着信先アドレスc'で検索をかける。すると、ステップ113で準備したエントリが変換情報テーブル510に見つかるため、着信先アドレス“c'”を“y+c”に変換する。送信元アドレスは、データを受信した回線番号に対応する仮想的なIPv6プレフィックスαを付加した「送信元仮想IPv6アドレス」“α+a”に書き換える(132)。トランスレータ1aは着信先アドレスに“y+c”、送信元アドレスに“α+a”をそれぞれ設定したパケットを送信する(133)。トランスレータ

1bはこのパケットをデータパケット変換・処理部13に送る。ここでは、着信先アドレスから仮想IPv6プレフィックスyを削除する。送信元アドレス“α+a”をVPN5cの内部で一意に識別するため、IPv4アドレス“a1'”に変換する。このIPv4アドレスは、送信元アドレス“α+a”に対する仮想的なアドレスで、VPN5cの内部で使用されていないIPアドレスの集合から選ぶ。以降、このアドレスを「送信元仮想IPv4アドレス」と呼ぶ。

【0024】トランスレータ1bは、“α+a”と“a1'”の対応付け変換規則を作成し、変換情報記憶部11のVPN#3変換情報テーブル530に記憶する(134)。端末4cが着信先アドレスに“c”、送信元アドレスに“a1'”を設定したパケットを受信する(135)。端末4cは、端末4aへ向けて着信先アドレス“a1'”、送信元アドレス“c”を設定したIPパケットを送信する(136)。トランスレータ1bではこのパケットが到着するとデータパケット変換・処理部13に送る。ここでは、変換情報記憶部11にデータを受信した回線の番号と着信先アドレス“a1'”で検索をかける。すると、ステップ134で準備したエントリが変換情報テーブル530に見つかるため、着信先アドレスを“a1'”を“α+a”に変換する。送信元アドレスは、データを受信した回線番号に対応する仮想的なIPv6プレフィックスyを付加した送信元仮想IPv6アドレス“y+c”に書き換える(137)。トランスレータ1bは着信先アドレスに“α+a”、送信元アドレスに“y+c”を設定したパケットを送信する(138)。

【0025】トランスレータ1aは、このパケットが到着するとデータパケット変換・処理部13に送る。ここで、着信先アドレスから仮想IPv6プレフィックスαを削除する。変換情報記憶部11に着信先アドレスの仮想IPv6プレフィックス“α”と送信元アドレス“y+c”で検索をかける。すると、さきに準備したエントリが変換情報テーブル510に見つかるため、送信元アドレスを“y+c”から“c”に変換する(139)。

【0026】端末4aは着信先アドレスに“a”、送信元アドレスに“c”を設定したパケットを受信する(140)。

【0027】本発明の実施の形態によれば、トランスレータ1とDNS-ALG2が連携し、IP網6の仮想IPv6プレフィックスを活用することにより、プライベートIPv4アドレスを有するVPN間で相互通信を行うことが可能になる。

【0028】本発明の第2の実施の形態を図面を用いて説明する。

【0029】図16は、本発明の第2の実施例の網構成を示す。図1と比較すると、図16の網構成は「VPN5のDNSサーバ3とDNS-ALG2の通信がトランスレータ1を経由する」こと、「VPNの相互通信において、DNS-ALG2が次に問い合わせるDNSサーバに、上記DNS-ALG2内の別

IPv6アドレスが設定されている」ことを特徴とする。

【0030】本実施例において、DNS-ALG2は、トランスレータ1に接続されるVPN対応にIPv6アドレスを有するマルチホームノードである。本実施例におけるDNS-ALG2aは、次に問い合わせるDNSサーバがDNS問い合わせを送信したVPNに存在しない場合は、次に問い合わせるDNSサーバのアドレス情報として、DNS-ALG2aの他のIPv6アドレスが記憶されている。次に問い合わせるDNSサーバがDNS問い合わせを送信したVPN内に存在する場合は、次に問い合わせるDNSサーバのアドレス情報として、そのVPN内に存在するDNSサーバの仮想IPv6アドレスが記憶されている。この仮想IPv6アドレスは、“仮想プレフィックス+各VPNにおいて、DNSサーバに割り当てられたIPv4アドレス”で構成される。

【0031】本実施例におけるトランスレータ1は、VPN毎のDNS-ALGアドレス変換情報と、DNSのメッセージを含むパケットを監視する機能と、DNSのメッセージを含むパケットのアドレス変換機能をさらに備える。VPN毎のDNS-ALGアドレス変換情報は、VPN対応にDNS-ALGのIPv6アドレスとVPNの内部でDNS-ALGを識別するためDNS-ALGに割り当てられた仮想IPv4アドレスとの対応関係を管理する。

【0032】図17と図18に示すシーケンスに従って、図16のVPN5aに存在する端末4aがVPN5bに存在する端末4bと通信する場合について説明する。VPN5aとVPN5bは、トランスレータ1aに接続される。VPN5aとトランスレータ1aの間で送受信するパケットのアドレス変換と、VPN5bとトランスレータ1aの間で送受信するパケットのアドレス変換は、トランスレータ1aで行われる。図17と図18において、VPN5aとトランスレータ1aの間のアドレス変換機能をTR-0、VPN5bとトランスレータ1aの間のアドレス変換機能をTR-Tと記載する。

【0033】図14と図17の主な差分は、「トランスレータ1aがDNSのメッセージを含むパケットのアドレスを変換する」ことと、「DNS-ALG2aのIPv6アドレスがVPN毎に異なる」ことである。

【0034】以下、図17と図18について、詳細に説明する。端末4aは端末4bの名前(host Bとする)を解決するためにDNSサーバ3aに対してDNS問い合わせを行う(151)。DNSサーバ3a(IPv4アドレス“da4”)は、この名前host Bに対応するIPアドレスを知らないため、次のDNSサーバ(DNS-ALG2a、仮想IPv4アドレス“pa4”)に対してDNS問い合わせを行う(152)。

【0035】トランスレータ1aのTR-0は、DNSのメッセージを含むパケットを検出し、パケットを変換する(153)。着信先アドレスは、トランスレータ1aが備えるDNS-ALGアドレス変換情報を用いて、DNS-ALG2aのVPN5a用のIPv6アドレス“α6”に変換する。送信元アドレスは、仮想プレフィックス管理テーブル300を参

照し、VPN5a用の仮想IPv6プレフィックス“α”を付加する。トランスレータ1aのTR-0は、アドレスを変換したDNS問い合わせパケットをDNS-ALG2aに送信する(154)。

【0036】DNS-ALG2aは、名前host Bに対するIPアドレスを知らない場合、前記処理ルーチン60により、DNS問い合わせを変換し(155)、DNS問い合わせを転送する(156)。DNS問い合わせの転送先には、DNS-ALG2aに付与された別のIPv6アドレス(VPN5b用のIPv6アドレス“β6”)が設定されている。

【0037】VPN5b用のIPv6アドレス“β6”宛のDNS問い合わせを受信したDNS-ALG2aは、名前host Bに対するIPアドレスを知らない場合、前記処理ルーチン60により、変換したDNS問い合わせを次のDNSサーバ3b(仮想IPv6アドレス“β+db4”)に送信する(157、158)。

【0038】トランスレータ1aのTR-Tは、DNSのメッセージを含むパケットを検出し、パケットを変換する(159)。着信先アドレスから、仮想プレフィックスβを削除する。送信元アドレスは、トランスレータ1aが備えるDNS-ALGアドレス変換情報を用いて、VPN5b用のDNS-ALG2aのIPv6アドレス“β6”に対する仮想IPv4アドレス“pb4”に変換する。トランスレータ1aのTR-Tは、アドレスを変換したパケットをDNSサーバ3bに送信する(160)。

【0039】DNSサーバ3bは、名前host Bに対するIPv4アドレス“b”を応答する(161)。トランスレータ1aのTR-Tは、DNSのメッセージを含むパケットを検出し、パケットを変換する(162)。送信元アドレスに、VPN5bに対応する仮想プレフィックスβを付加する。着信先アドレスは、トランスレータ1aが備えるDNS-ALGアドレス変換情報を用いて“pb4”から“β6”に変換する。トランスレータ1aのTR-Tは、アドレスを変換したパケットをDNS-ALG2aに送信する(163)。

【0040】DNS-ALG2aは、名前host Bに対するIPv4アドレス“b”に仮想プレフィックスβを付加し、“β+b”に書き換える(164)。

【0041】DNS-ALG2aは、DNS-ALG2aのVPN5a用のIPv6アドレス“α6”宛に、RDATAに“β+b”を設定したDNS応答を送信する(165)。

【0042】DNS応答を受信したDNS-ALG2aは、以後の変換のためにIPv6アドレス“β+b”を着信先仮想IPv4アドレス“b'”に変換する(166)。このIPv4アドレスは名前host Bに対する仮想的なアドレスで、VPN5aで使用されていないIPアドレスの集合から選ぶ。

【0043】DNS-ALG2aは、DNSサーバ3a経由で端末4aに名前host Bに対する着信先仮想IPv4アドレス“b'”を送信する(169、171、172)。トランスレータ1aはDNS応答169を検出すると、パケットを変換する(170)。着信先アドレスから、仮想プ

プレフィックス α を削除する。送信元アドレスは、トランスレータ1aが備えるDNS-ALGアドレス変換情報を用いて“ $\alpha 6$ ”から“pa4”からに変換する。トランスレータ1aのTR-0は、アドレスを変換したパケットをDNS3aに送信する(171)。

【0044】DNS-ALG2aは、“ $\beta + b$ ”と“b'”の対応付け変換規則を作成し、トランスレータ1aに送信する(167)。トランスレータ1aは、変換規則を変換情報記憶部11のVPN#1変換情報テーブル510に記憶し、DNS-ALG2aに応答を送信する(168)。

【0045】図15と図18の主な差分は、「トランスレータ1は、着信先アドレスと送信元アドレスの変換を行い(182)、パケットをトランスレータ内でルーティングし(184)、再び着信先アドレスと送信元アドレスの変換を行う(185)」ことである。

【0046】端末4aは端末4bへ向けてIPパケットの送信を始める。これらのパケットの着信先アドレスはb'、送信元アドレスは端末のIPv4アドレスaである(181)。

【0047】トランスレータ1aは、このパケットが到着するとデータパケット変換・処理部13に送る。ここでは、変換情報記憶部11にデータを受信した回線の番号と着信先アドレスb'で検索をかける。すると、ステップ167で準備したエントリが変換情報テーブル510に見つかるため、着信先アドレスを“b'”を“ $\beta + b$ ”に変換する。送信元アドレスには、データを受信した回線番号に対応する仮想的なIPv6プレフィックス α を付加する(182)。

【0048】トランスレータ1aは着信先アドレスに“ $\beta + b$ ”、送信元アドレスに“ $\alpha + a$ ”を設定したパケットを送信する(183)。このパケットは、トランスレータ1a内でルーティングされる(184)。

【0049】トランスレータ1aは、このパケットをデータパケット変換・処理部13に送る。ここでは、着信先アドレスから仮想IPv6プレフィックス β を削除する。トランスレータ1aは、送信元アドレス“ $\alpha + a$ ”をIPv4アドレス“a'”に変換する。このIPv4アドレスは、IPv6アドレス“ $\alpha + a$ ”に対する仮想的なアドレスで、VPN5bで使用されていないIPアドレスの集合から選ぶ。

【0050】トランスレータ1aは、“ $\alpha + a$ ”と“a'”の対応付け変換規則を作成し、変換情報記憶部11のVPN#2変換情報テーブル520に記憶する(185)。

【0051】端末4bは、着信先アドレスに“b'”、送信元アドレスに“a'”を設定したパケットを受信する(186)。

【0052】端末4bは、端末4aへ向けて着信先アドレス“a'”、送信元アドレス“b'”を設定したパケットを送信する(187)。

【0053】トランスレータ1aはこのパケットが到着

するとデータパケット変換・処理部13に送る。ここで、変換情報記憶部11にデータを受信した回線の番号と着信先アドレス“a'”で検索をかける。すると、ステップ185で準備したエントリが変換情報テーブル520に見つかるため、着信先アドレス“a'”を“ $\alpha + a$ ”に変換する。送信元アドレスには、データを受信した回線番号に対応する仮想的なIPv6プレフィックス“ β ”を付加する(188)。

【0054】トランスレータ1aは着信先アドレスに“ $\alpha + a$ ”、送信元アドレスに“ $\beta + b$ ”を設定したパケットをトランスレータ1a内でルーティングする(189、190)。

【0055】トランスレータ1aは、このパケットをデータパケット変換・処理部13に送る。着信先アドレス“ $\alpha + a$ ”から仮想IPv6プレフィックス α を削除する。ここで、変換情報記憶部11に着信先の仮想IPv6プレフィックス α と送信元アドレス“ $\beta + b$ ”で検索をかけると、さきに準備したエントリが変換情報テーブル510に見つかるため、送信元アドレスを“ $\beta + b$ ”から“b'”に変換する(191)。

【0056】端末4aは着信先アドレスに“a”、送信元アドレスに“b'”を設定したパケットを受信する(192)。

【0057】本発明の実施の形態によれば、トランスレータとDNS-ALGの連携と、仮想IPv6プレフィックスの活用により、複数のVPNが接続されているトランスレータはアドレスが重複する場合であっても、プライベートIPv4アドレスを有する端末を一意に識別できる。従って、プライベートIPv4アドレスを有するVPN間で相互通信が可能になる。

【0058】また、VPN毎のDNS-ALGを1つの物理装置に縮退することにより、VPN間でDNS-ALG装置を共有することが可能になる。

【0059】本発明の第3の実施の形態を図面を用いて説明する。

【0060】図19は、本発明の第3の実施例の網構成を示す。図16と比較すると、本実施例は、「複数のVPNがDNS-ALGを共有する」と、「複数のトランスレータがDNS-ALGを共有する」ことを特徴とする。本実施例におけるDNS-ALG2aは、ドメイン毎に名前解決の転送先を別々に設定する機能を備える。具体的には、次に問い合わせるDNSサーバのアドレス情報として、各VPNのドメイン名とそのVPNに存在するDNSサーバの仮想IPv6アドレスの対応関係を管理する。この仮想IPv6アドレスは、“仮想プレフィックス+各VPNにおいて、DNSサーバに割り当てられたIPv4アドレス”で構成する。

【0061】DNS-ALG2aは、処理ルーチン60のかわりに、名前hostBのQTYPEの値にかかわらず、“A”及び“AAAA”で名前解決を行う機能を備える。本実施例におけるトランスレータ1は、実施例1におけるトランス

レータ1の機能に加え、DNS-ALGアドレス変換情報と、DNSのメッセージを含むパケットを監視する機能と、DNSのメッセージを含むパケットのアドレス変換機能を備える。

【0062】DNS-ALGアドレス変換情報は、DNS-ALGのIPv6アドレスとVPNの内部でDNS-ALGを識別するためDNS-ALGに割り当てられた仮想IPv4アドレスとの対応関係を管理する。

【0063】以下、VPN5aに存在する端末4aがVPN5bに存在する端末4bの名前を解決する場合について説明する。

【0064】本実施例において、トランスレータ1aはDNS-ALG2aのIPv6アドレス“alg6”とVPN毎にVPNの内部でDNS-ALGを識別するためにDNS-ALG2aに割り当てられた仮想IPv6の対応関係を保持する。

【0065】端末4aは端末4bの名前(hostBとする)のアドレスを得るためにDNS問い合わせを行う。DNSサーバ3aは名前hostBを解決できないため、次のDNSサーバ(DNS-ALG2a)にDNS問い合わせを送信する。このDNS問い合わせのパケットヘッダの着信先アドレスにはDNS-ALG2aに対してVPN5aで割り当てられた仮想IPv4アドレス“pa4”が、送信元アドレスにはDNS3aのIPv4アドレス“da4”が設定される。

【0066】トランスレータ1aがこのDNS問い合わせを検出すると、DNS-ALGアドレス変換情報を参照して着信先アドレスを“pa4”からDNS-ALG2aのIPv6アドレス“alg6”に変換する。送信元アドレスには、VPN5a用のIPv6プレフィックス α を付加し、“ $\alpha + da4$ ”に書きかえる。

【0067】上記DNS問い合わせを受信したDNS-ALG2aは、名前hostBに対するIPアドレスを知らない場合、次のDNSサーバに問い合わせる。ここで、名前hostBを解決するために、次に問い合わせるべきDNSサーバとして、仮想IPv6アドレス“ $\beta + db4$ ”が設定される。“ $\beta + db4$ ”は、VPN5bのDNSサーバ3bの仮想IPv6アドレスである。

【0068】DNS-ALG2aは、DNS問い合わせをDNSサーバ3bに送信し、応答を待つ。このDNS問い合わせの送信元アドレスにはDNS-ALG2aのIPv6アドレス“alg6”が、着信先アドレスには“ $\beta + db4$ ”が設定される。

【0069】トランスレータ1aは、上記DNS問い合わせのパケットを検出し、VPN毎のDNS-ALGアドレス変換情報を用いて送信元アドレスを、DNS-ALG2aのIPv6アドレス“alg6”をVPN5b内でDNS-ALG2aを識別する仮想IPv4アドレス“pb4”に変換する。着信先アドレスはプレフィックス β を削除し、“ $\beta + db4$ ”から“db4”に書き換える。

【0070】DNSサーバ3bは、DNS-ALG2aに、名前hostBに対するIPv4アドレス“b”を応答する。

【0071】DNS-ALG2aは、以後の変換のためにIPv4

アドレス“b”を着信先仮想IPv6アドレス“ $\beta + b$ ”に書き換えたのち、“ $\beta + b$ ”を着信先仮想IPv4アドレス“b'”に変換する。上記IPv4アドレス“b'”は名前hostBに対する仮想的なアドレスで、VPN5aで使用されていないIPアドレスの集合から選ぶ。

【0072】DNS-ALG2aは、DNSサーバ3a経由で端末4aに名前hostBに対する着信先仮想IPv4アドレス“b'”を送信する。

【0073】以降の処理の流れは、第2の実施例と同じである。

【0074】本発明の実施の形態によれば、DNS-ALGがマルチホームノードでない場合であっても、VPN間でDNS-ALGを共用でき、さらにDNS-ALGにおける処理を軽減できる。

【0075】本発明の第4の実施の形態を図面を用いて説明する。

【0076】図20は、本発明の第4の実施例の網構成を示す。図16と比較すると、図20の網構成は、「L2SW7がVPN5毎に存在するトランスレータの回線(17a、17b)を多重する」ことを特徴とする。本実施例におけるL2SW7は、図21に示すVPN管理テーブル320を備える。

【0077】図21は、VPN管理テーブル320のテーブル構成を示す。本テーブルは、MACアドレスやIEEE 802.1QのTAG IDに代表されるレイヤ2(L2)情報毎に生成された複数のエントリ(320-1~320-n)からなる。各エントリは、L2情報321対応に、VPN識別子322と、対トランスレータの回線番号323を定義する。

【0078】本実施例において、VPN5aからパケットを受信したL2SW7は、VPN管理テーブル320を受信パケットのL2情報(例えば、送信元MACアドレスや、IEEE 802.1QのTAG ID)で検索する。L2SW7は、VPN5aに対応する回線17aからトランスレータ1aにパケットを送信する。

【0079】本発明の実施の形態によれば、トランスレータが回線対応に収容するVPNをL2SWで多重することができる。

【0080】本発明の第5の実施の形態を図面を用いて説明する。

【0081】図22は、本発明の第5の実施例の網構成を示す。図16と比較すると、図22の網構成は、「トランスレータ1aの回線17aに複数のVPN(5a、5b)が収容される」とこと、「トランスレータ1aが図9に示す仮想プレフィックス管理テーブル300のかわりに図10に示す仮想プレフィックス管理テーブル310を備え、L2情報からVPNを識別する」ことを特徴とする。

【0082】図10は、仮想プレフィックス管理テーブル310のテーブル構成を示す。本テーブルは、MACアドレスやIEEE 802.1QのTAG IDに代表されるレイヤ2(L

2) 情報毎に生成された複数のエントリ (310-1 ~ 310-n) からなる。各エントリは、L2情報311に対応に、VPN識別子312と、仮想プレフィックス313を定義する。

【0083】本実施例において、VPN5aからパケットを受信したトランスレータ1aは、仮想プレフィックス管理テーブル310を受信パケットのL2情報(例えば、送信元MACアドレスやIEEE 802.1Q TAG ID)で検索する。すると、L2情報に対応する仮想プレフィックスαが仮想プレフィックス管理テーブル310に見つかる。トランスレータ1aは、仮想プレフィックスによりVPNを識別する。

【0084】本発明の実施の形態によれば、トランスレータの1つの回線に複数のVPNを収容できる。

【0085】

【発明の効果】以上の実施の形態から明らかなように、本発明はIPv6ベースのDNS-ALGとトランスレータの連携によって、従来のTwice NATによるアドレス変換で必要な変換情報を動的に作成する場合に必要であった、着側の端末に対する仮想アドレスを生成するDNS-ALGの処理負荷の軽減と大容量変換テーブルの削減を可能にする。

【0086】本発明によるトランスレータとDNS-ALGをプロバイダが一括管理し、トランスレータに複数のVPNを収容すれば、既存のVPNを置きかえることなく、VPN間の相互接続が可能になる。

【図面の簡単な説明】

【図1】本発明の第1の実施例であるIP網を介したVPNの相互接続構成を示すブロック図。

【図2】トランスレータ1の一例のブロック図。

【図3】DNS-ALG2の一例のブロック図。

【図4】IPv4パケットのフォーマット図。

【図5】IPv6パケットのフォーマット図。

【図6】DNS問い合わせのフォーマット図。

【図7】DNS応答のフォーマット図。

【図8】DNS応答の詳細フォーマット図。

【図9】トランスレータ1が備える仮想プレフィックス管理テーブルのテーブル図。

【図10】本発明の第5の実施例において、トランスレー

タ1が備える仮想プレフィックス管理テーブルのテーブル図。

【図11】トランスレータ1が備える変換情報テーブルのテーブル図。

【図12】DNS-ALG2が備えるDNSメッセージ変換処理ルーチンの流れ図。

【図13】DNS-ALG2が備えるDNSメッセージ変換処理ルーチンの流れ図。

【図14】本発明の第1の実施例における名前解決のシーケンス図。

【図15】本発明の第1の実施例におけるVPNが相互通信する場合のシーケンス図。

【図16】本発明の第2の実施例であるトランスレータに複数のVPNが接続される場合の網構成を示すブロック図。

【図17】本発明の第2の実施例における名前解決のシーケンス図。

【図18】本発明の第2の実施例におけるVPNが相互通信する場合のシーケンス図。

【図19】本発明の第3の実施例である複数のVPNが1つのDNS-ALG装置を利用する場合の網構成を示すブロック図。

【図20】本発明の第4の実施例であるL2SW7がVPNを多重する場合の網構成を示すブロック図。

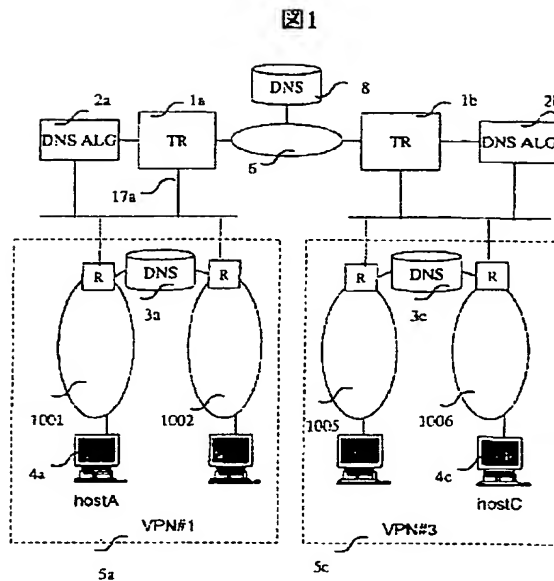
【図21】本発明の第4の実施例において、L2SW7が備えるVPN管理テーブルのテーブル図。

【図22】本発明の第5の実施例であるトランスレータ1がL2情報を活用してVPNを識別する場合の網構成を示すブロック図。

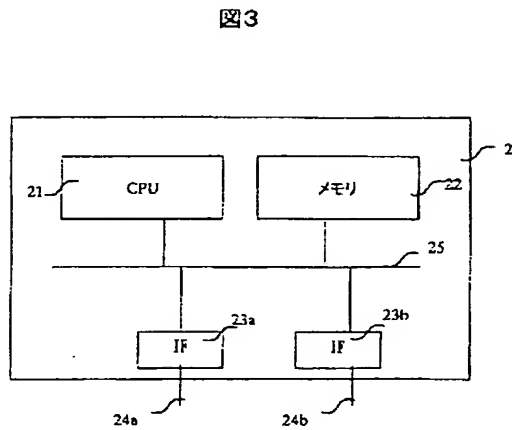
【符号の説明】

1 トランスレータ、2 DNS-ALG、3 VPN5が備えるDNSサーバ、4 VPNの端末、5 VPN、6 IP網、7 L2SW、8 IP網6が備えるDNSサーバ、31 送信元IPv4アドレス、32 着信先IPv4アドレス、33 IPv4ペイロード、34 送信元IPv6アドレス、35 着信先IPv6アドレス、36 IPv6ペイロード、41 DNSメッセージヘッダ部、42 DNS問い合わせ部、43 DNS応答部、60 DNS変換処理ルーチン。

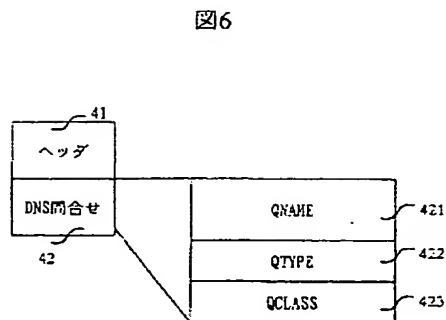
【図1】



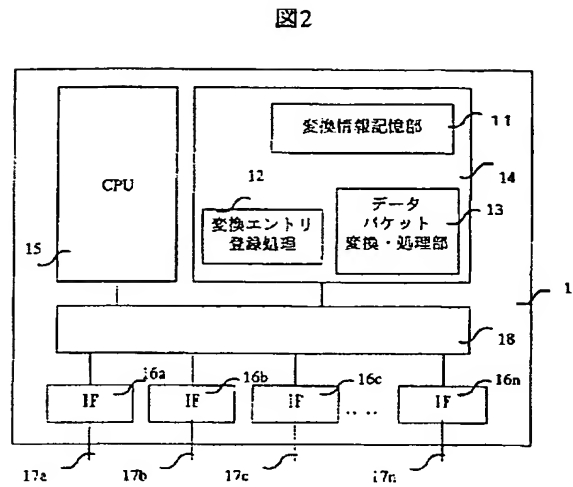
【図3】



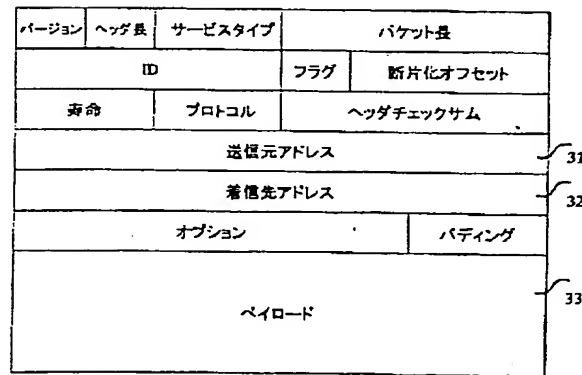
【図6】



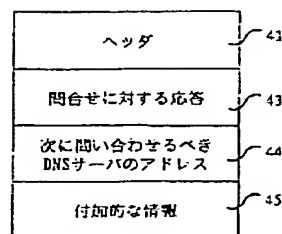
【図2】



【図4】



【図7】



【図9】

300 仮想プレフィックス管理テーブル

301 回数番号	302 仮想プレフィックス	303 ポインタ
xxx	α	p1
xyy	β	p2
...		
...		

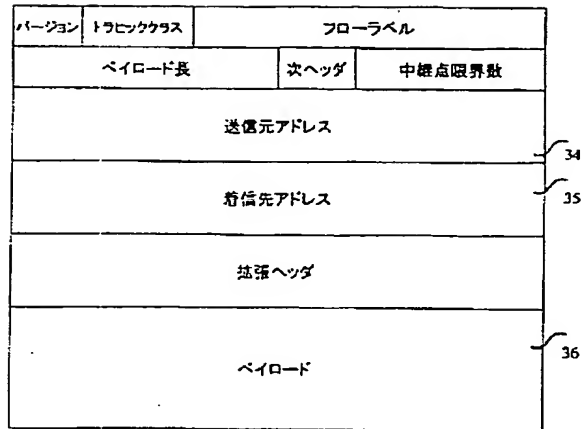
300-1

300-2

300-n

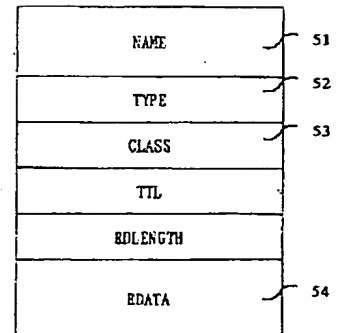
【図5】

図5



【図8】

図8



【図10】

図10

310 仮想プレフィックス管理テーブル

311 L2情報	312 VPN識別子	313 仮想プレフィックス	
aaa	1	α	310-1
bbb	2	β	310-2
⋮			310-n

【図21】

図21

320 VPN管理テーブル

321 L2情報	322 VPN識別子	323 回線番号	
aaa	1	xxx	320-1
bbb	2	yyy	320-2
⋮			320-n

【図11】

図11

500 変換情報テーブル

510 VPN#1 変換情報テーブル

501 V4アドレス	502 V6アドレス	
b'	$\beta + b$	510-1
c'	$\gamma + c$	510-2
⋮		510-n

520 VPN#2 変換情報テーブル

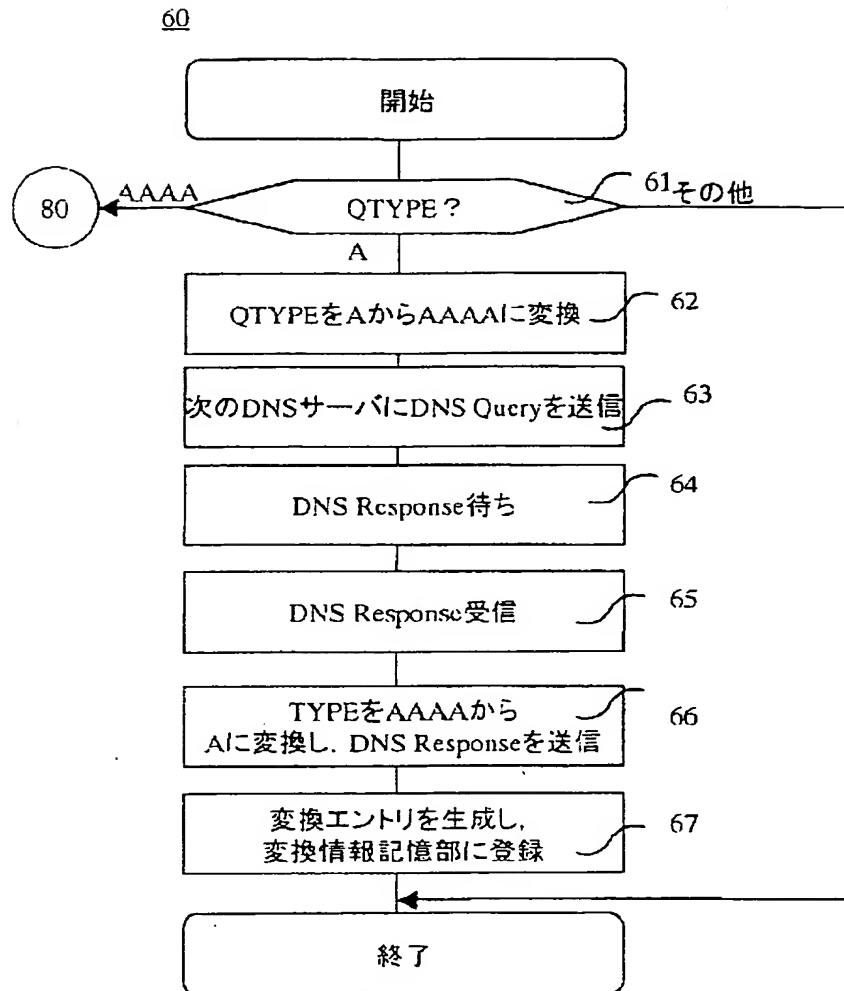
501 V4アドレス	502 V6アドレス	
a'	$\alpha + a$	520-1
⋮		520-n

530 VPN#3 変換情報テーブル

501 V4アドレス	502 V6アドレス	
a1'	$\alpha - a$	530-1
⋮		530-n

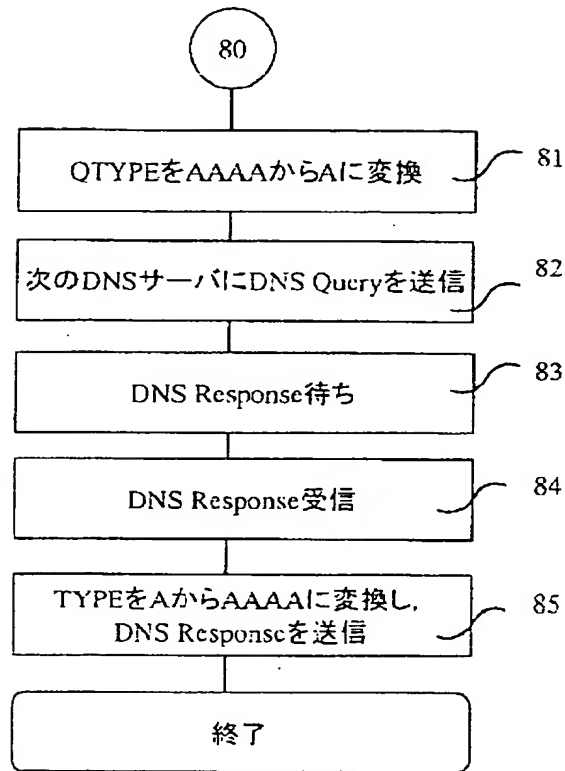
【図12】

図12



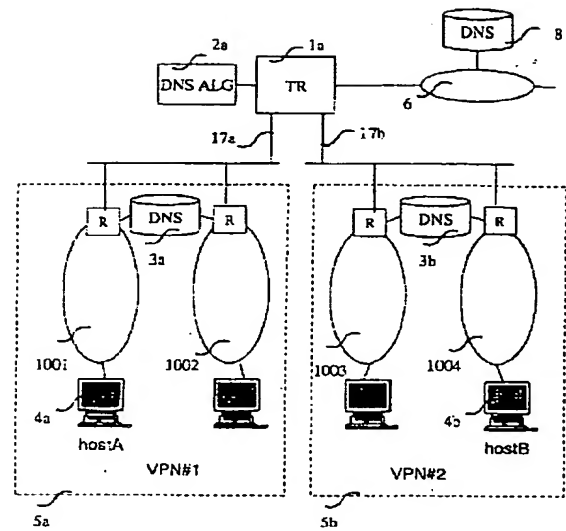
【図13】

図13



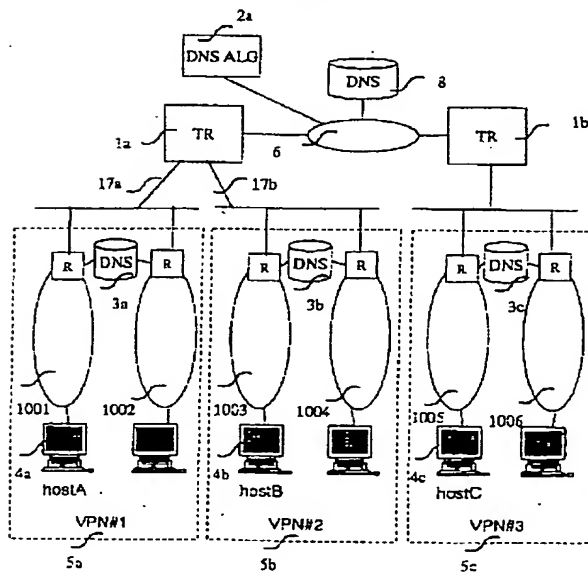
【図16】

図16



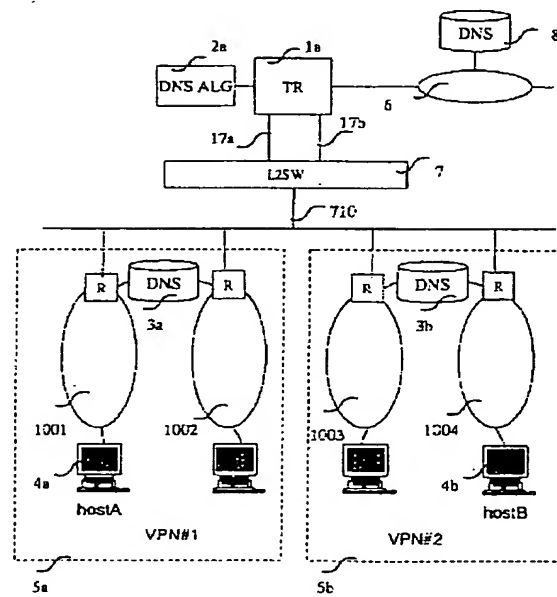
【図19】

図19



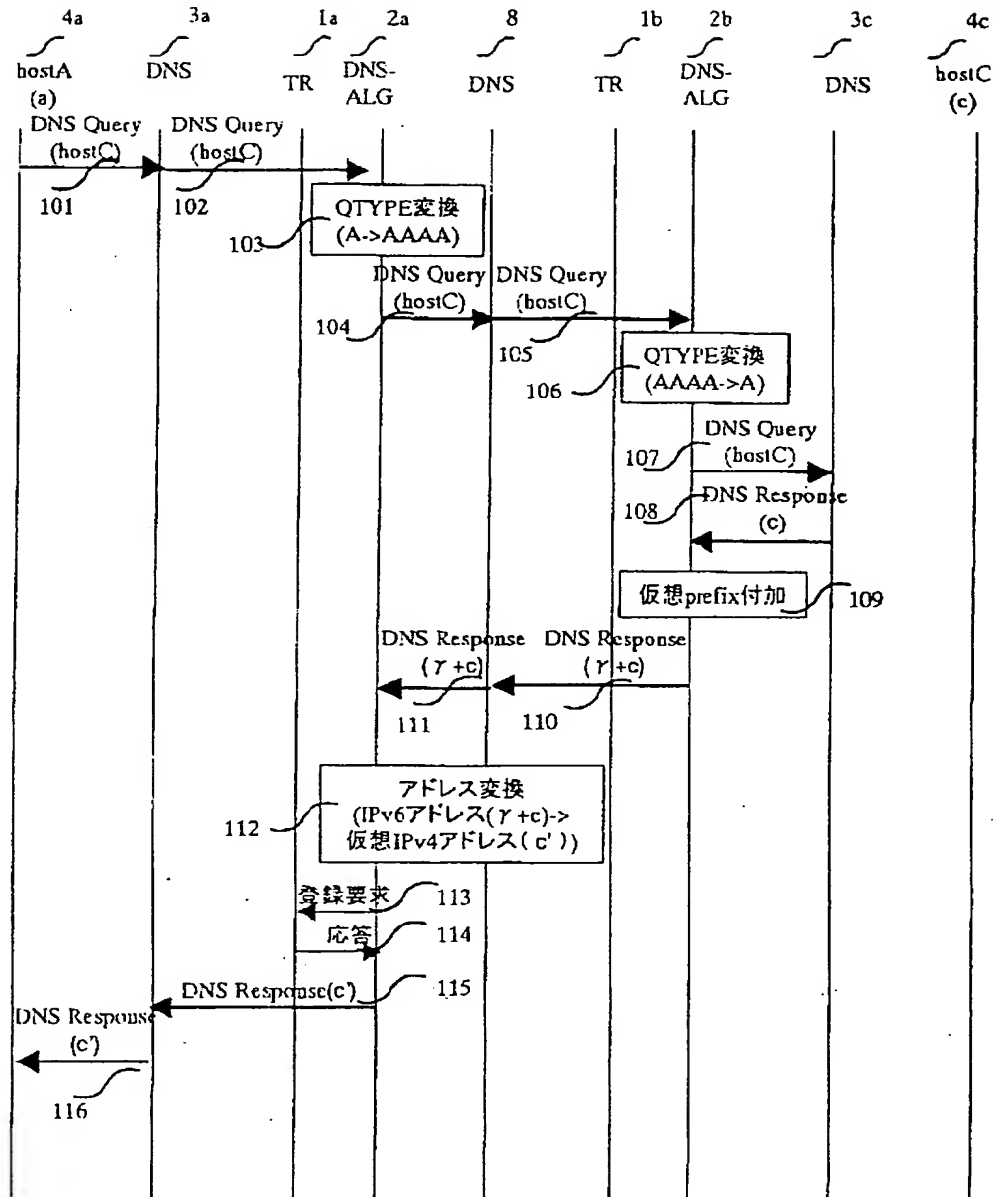
【図20】

図20



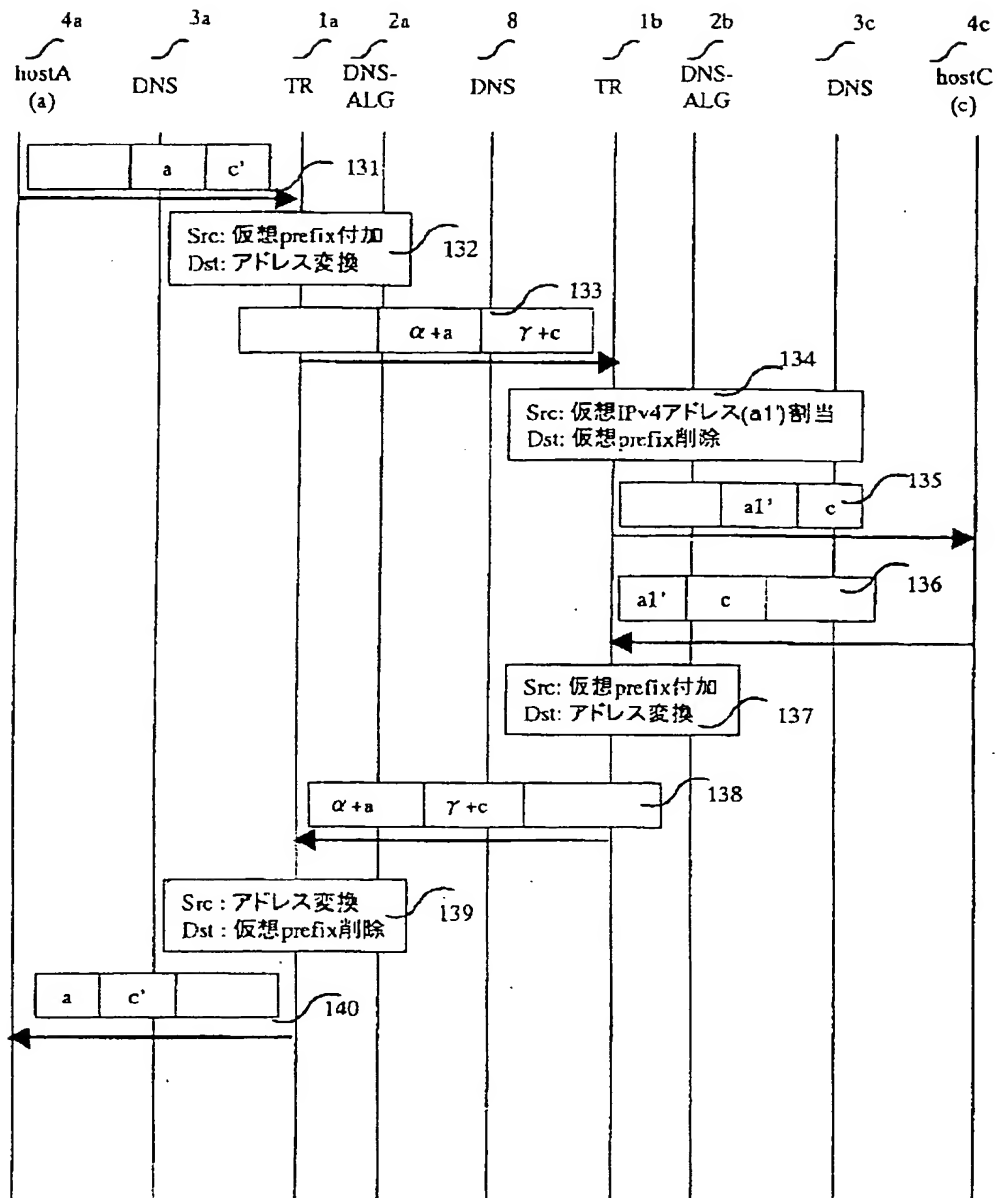
【図14】

図14

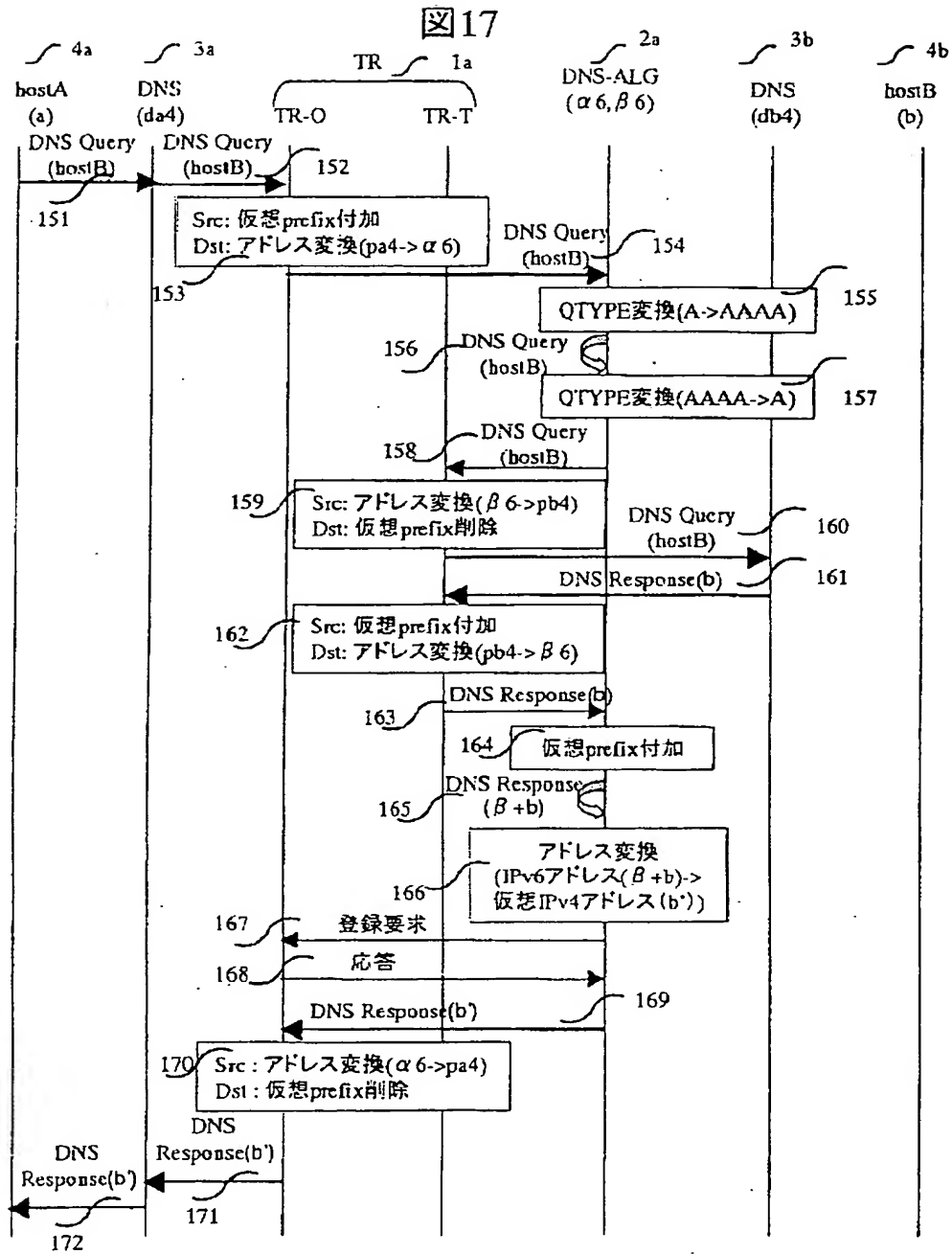


【図15】

図15

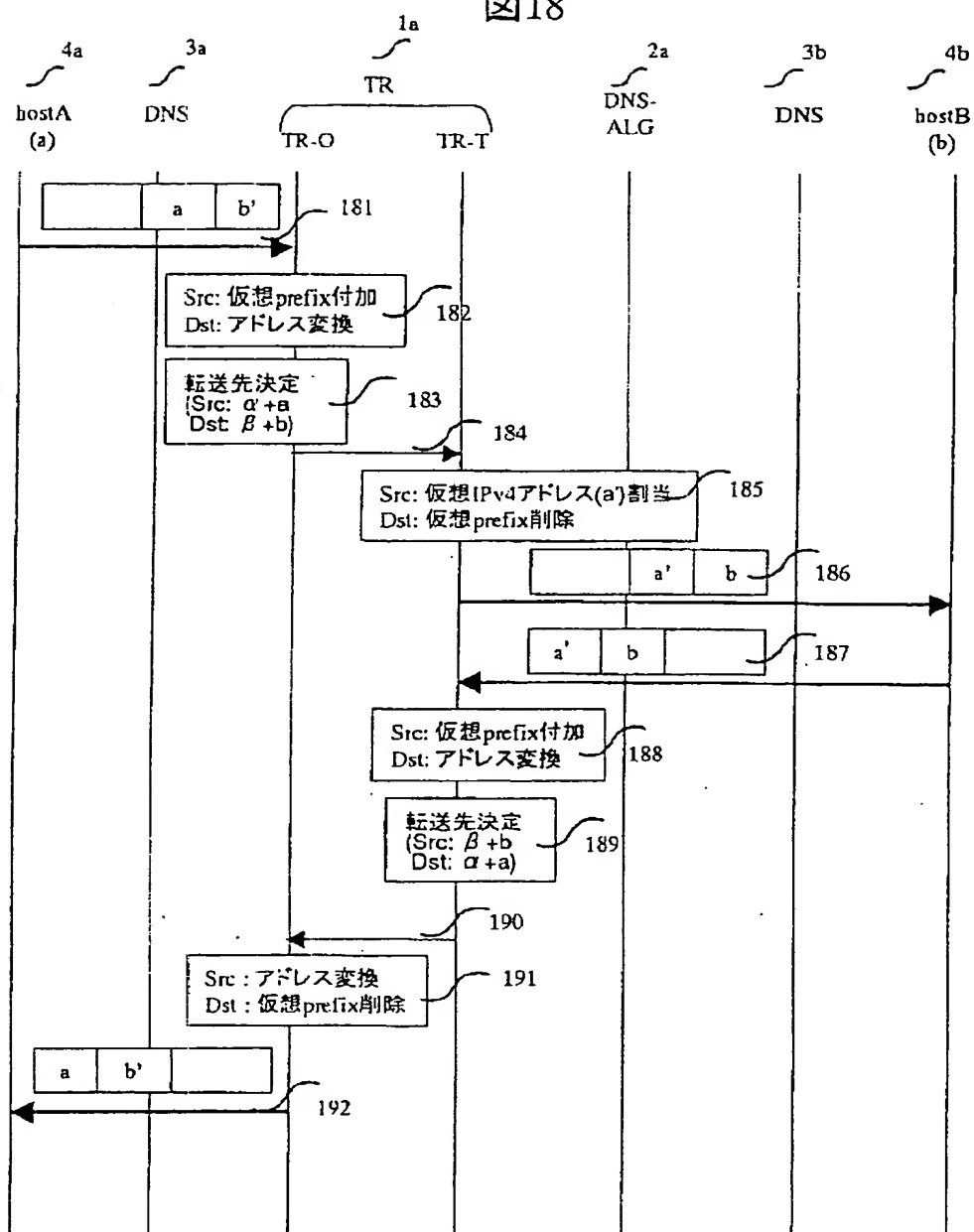


【図17】



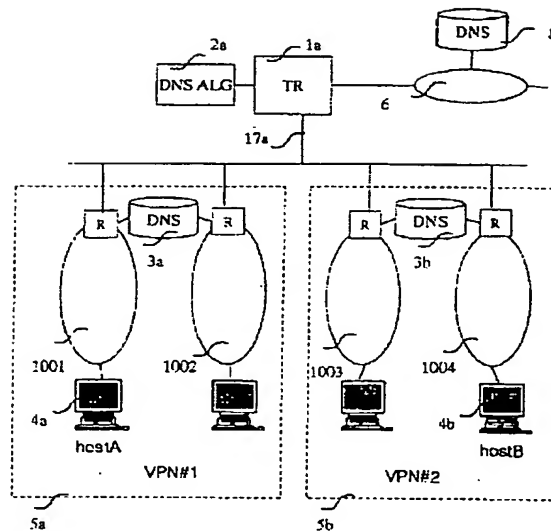
【図18】

図18



【図22】

図22



フロントページの続き

(72)発明者 林 匡哉
 東京都国分寺市東恋ヶ窪一丁目280番地
 株式会社日立製作所中央研究所内
 (72)発明者 竹内 敬亮
 東京都国分寺市東恋ヶ窪一丁目280番地
 株式会社日立製作所中央研究所内

(72)発明者 妹尾 高光
 神奈川県横浜市戸塚区戸塚町216番地 株
 式会社日立製作所通信事業部内
 F ターム(参考) 5B089 GA31 GB01 KB06 KF05 KH03
 5K030 GA14 HA08 HB21 HC01 HC13
 HD03 JA11 JT03 KA04 LB13
 LE02 MD08 MD10
 5K034 AA10 AA20 DD03 EE10 HH61